IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently amended) An interface security system between devices connected to each other and transmitting/receiving a signal, the interface security system comprising:

a first device transmitting/receiving a signal, the first device including:

a first selector selecting a connection pattern between the signal transmitted/received and a first external terminal configured to transmit/receive the signal based on a switch signal, the first selector including [[and]] a first switch switching a connection between the signal and the first external terminal in accordance with the connection pattern selected by the first selector, and

a first counter configured to generate counter values in synchronization between the first and second devices and to send the counter values to the second selector, the counter values being used for deciding a connection pattern; and

a second device connected to said first device and configured to transmit/receive a signal, the second device including:

a second selector configured to select ~~selecting~~ a connection pattern between the signal transmitted/received and a second external terminal configured to transmit/receive the signal based on a switch signal, the second selector including [[and]] a second switch configured to switch ~~switching~~ a connection between the signal and the second external terminal in accordance with the connection pattern selected by the second selector, and

a second counter configured to generate counter values in synchronization between the first and second devices and to send the counter values to the first selector, the counter values being used for deciding a connection pattern; wherein

the second selector inputs a switch signal of the same value as the switch signal that the [second] first selector inputs, and

the first and second selectors decide connection patterns, respectively, based on the counter values that the first and second counters generate.

2. (Canceled)

3. (Currently amended) [[The]] An interface security system ~~according to claim 1, wherein: said first device and said second device include first and second pseudo-random number generators generating pseudo-random number sequences using mutually common seeds of random numbers as initial values, respectively~~ between devices connected to each other and transmitting/receiving a signal, the interface security system comprising:

a first device configured to transmit/receive a signal, the first device including:

a first selector configured to select a connection pattern between the signal transmitted/received and a first external terminal configured to transmit/receive the signal based on a switch signal, the first selector including a first switch configured to switch a connection between the signal and the first external terminal in accordance with the connection pattern selected by the first selector,

a first bidirectional buffer connected to the first external terminal, and

a first pseudo-random number generator configured to generate pseudo-random number sequences based on seeds of random numbers as initial values; and

a second device connected to said first device and configured to transmit/receive a signal, the second device including:

a second selector configured to select a connection pattern between the signal transmitted/received and a second external terminal configured to transmit/receive the signal

based on a switch signal, the second selector including a second switch switching a connection between the signal and the second external terminal in accordance with the connection pattern selected by the second selector,

a second bidirectional buffer connected to the second external terminal, and

a second pseudo-random number generator configured to generate pseudo-random number sequences based on the seeds of random numbers as initial values; wherein

the second selector inputs a switch signal of the same value as the switch signal that the first selector inputs,

the first and second selectors control the first and second bidirectional buffers, respectively, so as to switch the directions of the input/output of the first and second external terminals in accordance with the connection pattern, and

the first and second selectors decide connection patterns, respectively, based on the pseudo-random number sequences that the first and second pseudo-random number generators generate.

4. (Original) The interface security system according to claim 3, wherein:

said first device includes a seed generator generating a seed of the random number and sending it to the first pseudo-random number generator and the second pseudo-random number generator; and

the first and second pseudo-random number generators generate the pseudo-random number sequences using the seed of the random number that the seed generator generates as an initial value.

5. (Original) The interface security system according to claim 4, wherein:

said first device includes a cryptography circuit encrypting the seed of the random number that the seed generator generates in a predetermined cryptography mode and transferring it to the second device; and

said second device includes a decode circuit decoding the encrypted seed of the random number transferred from the first device in a predetermined cryptography mode and sending it to the second pseudo-random number generator.

6. (Original) The interface security system according to claim 4, wherein:

the seed generator is provided in the external of the first device and the second device; and

the seed generator delivers the generated seed to the random number to first and second pseudo-random number generators of the first and second devices.

7. (Currently Amended) The interface security system according to claim [1] 3, wherein:

said first device includes a physical random number generator generating a physical random number from electrical noise inputted from a noise source and sending the physical random number to both of the first selector of the first device and the second selector of the second device; and

the first and second selectors of the first and second devices decide a connection pattern based on the physical random number sequence.

8. (Canceled)

9. (Currently Amended) The interface security system according to claim [1] 3, wherein

the first and second selectors select the connection pattern and switch the connection at a predetermined time interval.

10. (Currently Amended) The interface security system according to claim [1] 3, wherein

the first and second selectors select the connection pattern and switch the connection each time the signal is transmitted/received between the first and second devices.

11. (Currently Amended) The interface security system according to claim [1] 3, wherein said first and said second devices are semiconductor devices which are resin sealed, respectively.

12. (Currently Amended) An interface security method between first and second devices connected to each other and transmit/receive a signal, the interface security method comprising:

selecting a connection pattern between a signal transmitted/received and a first external terminal in the first device configured to transmit/receive the signal based on a switch signal;

switching a connection between the signal and the first external terminal in accordance with the connection pattern selected;

selecting a connection pattern between a signal transmitted/received and a second external terminal in the second device configured to transmit/receive the signal based on a switch signal having the same value as that of the switch signal of the first device;

switching a connection between the signal and the second external terminal in accordance with the connection pattern selected; and

generating counter values in synchronization between the first and second devices, and wherein said selection of the connection patterns in the first and second devices is based on the counter values.

13. (Canceled)

14. (Currently Amended) [[The]] An interface security method ~~according to claim 12, further~~ between first and second devices connected to each other to transmit/receive a signal, the interface security method comprising:

selecting a connection pattern between a signal transmitted/received and a first external terminal in the first device configured to transmit/receive the signal based on a switch signal;

switching a connection between the signal and the first external terminal in accordance with the connection pattern selected;

selecting a connection pattern between a signal transmitted/received and a second external terminal in the second device configured to transmit/receive the signal based on a switch signal having the same value as that of the switch signal of the first device;

switching a connection between the signal and the second external terminal in accordance with the connection pattern selected;

controlling bidirectional buffers connected to the external terminals of the first and second devices so as to switch the directions of the input/output of the first and second external terminals in accordance with the connection pattern; and

generating pseudo-random number sequences using mutually common seeds of random numbers as initial values in the first and second devices, wherein said selection of the connection patterns in the first and second devices is based on the pseudo-random number sequences, respectively.

15. (Original) The interface security method according to claim 14, further comprising generating a seed of a random number in the first device and transferring it to the second device, wherein said pseudo-random number sequences in the first and second devices are generated using said seed of the random number as an initial value, respectively.

16. (Original) The interface security method according to claim 15, further comprising:

encrypting the seed of the random number that the seed generation step generates in a predetermined cryptography mode in the first device and transmitting it to the second device; and

decoding the encrypted seed of the random number transferred from the first device in a predetermine cryptography mode in the second device.

17. (Original) The interface security method according to claim 14, further comprising generating seed of a random number in the external and transferring it to both first device and second device, wherein said pseudo-random number sequences in the first and second devices are generated using said seed of the random number as an initial value, respectively.

18. (Currently Amended) The interface security method according to claim [12] 14, further comprising:

generating a physical random number from electrical noise inputted from a noise source; and

sending said physical random number to both first and second device, and wherein

said selection of the connection patterns in the first and second devices is based on the physical random number sequence.

19. (Canceled)

20. (Currently Amended) The interface security method according to claim [12] 14, wherein the selection of the connection patterns and the switching connection between the signal and the external terminal are performed at a predetermined time interval in the first and second devices.

21. (Currently Amended) The interface security method according to claim [12] 14, wherein the selection of the connection patterns and the switching connection between the signal and the external terminal are performed every time signal transmission/reception is performed between the first and second devices.

22. (New) An interface security system between devices connected to each other and transmitting/receiving a signal, the interface security system comprising:

a first device transmitting/receiving a signal, the first device including:

a first selector selecting a connection pattern between the signal transmitted/received and a first external terminal configured to transmit/receive the signal based on a switch signal, the first selector including a first switch switching a connection between the signal and the first external terminal in accordance with the connection pattern selected by the first selector; and

a second device connected to said first device and configured to transmit/receive a signal, the second device including:

a second selector configured to select a connection pattern between the signal transmitted/received and a second external terminal configured to transmit/receive the signal based on a switch signal, the second selector including a second switch configured to switch a connection between the signal and the second external terminal in accordance with the connection pattern selected by the second selector; wherein

the second selector inputs a switch signal of the same value as the switch signal that the first selector inputs,

the first device and the second device include first and second pseudo-random number generators generating pseudo-random number sequences using mutually common seeds of random numbers as initial values, respectively, and

the first and second selectors decide connection patterns, respectively, based on the pseudo-random number sequences that the first and second pseudo-random number generators generate.

23. (New) An interface security method between first and second devices connected to each other to transmit/receive a signal, the interface security method comprising:

selecting a connection pattern between a signal transmitted/received and a first external terminal in the first device configured to transmit/receive the signal based on a switch signal;

switching a connection between the signal and the first external terminal in accordance with the connection pattern selected;

selecting a connection pattern between a signal transmitted/received and a second external terminal in the second device configured to transmit/receive the signal based on a switch signal having the same value as that of the switch signal of the first device;

switching a connection between the signal and the second external terminal in accordance with the connection pattern selected; and

generating pseudo-random number sequences using mutually common seeds of random numbers as initial values in the first and second devices, wherein said selection of the connection patterns in the first and second devices is based on the pseudo-random number sequences, respectively.